IN THE CLAIMS:

This listing of claims replaces all prior versions, and listings, of claims of this application:

1 - 45. (Canceled)

46. (Currently amended) A method for providing authentication when messages are sent between an electronic communication apparatus and a server according to a synchronization protocol in which a plurality of different authentication methods, among which a subset comprises addition authentication methods, comprising:

providing an authentication method indicator that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed;

incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods; and

transmitting said message to said server according to an authentication protocol of the synchronization protocol.

47. (Previously presented) The method according to claim 46, wherein the authentication method indicator is incorporated into a meta command of the synchronization protocol.

48. (Previously presented) The method according to claim 46, wherein the message is an initialization message, and the authentication capabilities of the electronic communication apparatus is indicated in an authentication method list of the initialization message, which is sent to the server for establishing a connection.

49. (Previously presented) The method according to claim 46, wherein any

authentication data relating to the specified authentication method is incorporated in a data string of the message sent according to the synchronization protocol.

50. (Previously presented) The method according to claim 46, wherein the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication.

51. (Previously presented) The method according to claim 46, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides server authentication.

52. (Previously presented) The method according to claim 46, wherein the authentication method is Wireless Public Key Infrastructure (WPKI) or Wireless Identity Module (WIM) authentication.

53. (Previously presented) The method according to claim 46, wherein the authentication method is SecureId or SafeWord authentication.

54. (Previously presented) The method according to claim 48, further comprising:

determining at the server the authentication capabilities of the electronic communication apparatus based on the plurality of authentication capabilities listed in the authentication method list.

55. (Previously presented) The method according to claim 54, further comprising:

executing at the server authentication operations according to one of the plurality of authentication capabilities indicated in the authentication method list;

preparing a message at the server comprising the authentication method indicator and any authentication data relating to the specified authentication method; and

transmitting the message to the electronic communication apparatus.

56. (Previously presented) The method according to claim 55, further comprising:

receiving the message at the electronic communication apparatus;

executing, at the electronic communication apparatus, authentication operations according to the authentication method indicated by the authentication method indicator to generate an expected result;

preparing a response to the server comprising the authentication method indicator, and any authentication data; and

transmitting the response to the server.

57. (Previously presented) The method according to claim 46, wherein the authentication method is Subscriber Identity Module/Universal Subscriber Identity Module (SIM/USIM) authentication, the method further comprising:

using CKs/IKs (cipher keys/integrity keys) generated by the electronic communication apparatus and the server, respectively, to provide integrity protection, wherein the CKs/IKs are used for generating MAC values; and

using a hashing function for computing a Hashed Method Authentication Code (HMAC) on the message.

58. (Previously presented) The method according to claim 52, further comprising:

generating, at the server, an integrity key that is encrypted with the public key of the electronic communication apparatus;

sending the integrity key to the electronic communication apparatus;

using the integrity key at the electronic communication apparatus to generate MAC values; and

using a hashing function at the electronic communication apparatus to compute a Hashed Method Authentication Code (HMAC) on the message.

59. (Currently amended) An electronic communication apparatus, comprising:

means for synchronizing via a synchronization protocol in which a plurality of different authentication methods are available, among which a subset comprises addition authentication methods;

means for providing an authentication method indicator that specifies an authentication method of the plurality of different authentication methods according to which the authentication is to be executed;

means for incorporating into a message the authentication method indicator comprising a plurality of authentication capabilities of the communication apparatus among the plurality of different authentication methods; and

means for transmitting said message to a server according to an authentication protocol of [[a]]the synchronization protocol.

60. (Previously presented) The electronic communication apparatus according to claim 59, further comprising:

means for sending an initialization message to the server for establishing a connection, the message comprising the authentication method indicator.

61. (Previously presented) The electronic communication apparatus according to claim 60, wherein the initialization message further comprises type of apparatus and/or identity of the electronic communication apparatus.

62. (Previously presented) The electronic communication apparatus according to claim 61, further comprising:

means for incorporating authentication data in a data string of the message to be sent according to the synchronization protocol.

63. (Previously presented) The electronic communication apparatus according to claim 59, further comprising:

means for using an IK (integrity key) to generate a MAC to provide integrity

protection; and

means for using a hashing function to compute a Hashed Method Authentication Code (HMAC) on the message to be sent.

64. (Previously presented) The electronic communication apparatus according to claim 59, wherein the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication.

65. (Previously presented) The electronic communication apparatus according to claim 59, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides server authentication.

66. (Previously presented) The electronic communication apparatus according to claim 59, wherein the authentication method is SecureId, SafeWord, Wireless Public Key Infrastructure (WPKI) and/or Wireless Identity Module (WIM) authentication.

67. (Previously presented) The electronic communication apparatus according to claim 59, wherein the electronic communication apparatus is a pager, an electronic organizer, and/or a smartphone.

68. (Previously presented) The electronic communication apparatus according to claim 59, wherein the electronic communication apparatus is a mobile telephone.

69. (Currently amended) A server for synchronizing by a synchronization protocol in which a plurality of different authentication methods are available, among which a subset comprises addition authentication methods, the server comprising:

means for incorporating an authentication method indicator in a message to be sent according to an authentication protocol of a synchronization protocol for indicating an

authentication method of the plurality of different authentication methods according to which the authentication is to be executed;

means for determining from the authentication method indicator of a received message, a plurality of authentication capabilities of an apparatus among the plurality of different authentication methods; and

electronic apparatus for determining the authentication method to use based on the plurality of authentication capabilities.

70. (Previously presented) The server according to claim 69, further comprising:

means for incorporating any authentication data in a data string of a message to be transmitted according to the synchronization protocol.

71. (Previously presented) The server according to claim 69, further comprising:

means for executing authentication according to the determined authentication method.

72. (Previously presented) The server according to claim 69, further comprising:

means for using an IK (integrity key) to generate a MAC to provide integrity protection; and

means for using a hashing function to compute a Hashed Method Authentication Code (HMAC) on the message to be sent.

73. (Previously presented) The server according to claim 70, wherein the authentication method is Global System for Mobile communications (GSM) Subscriber Identity Module (SIM) authentication.

74. (Previously presented) The server according to claim 69, wherein the authentication method is Universal Mobile telephone System (UMTS) Universal Subscriber Indentity Module (USIM) authentication, which provides a server authentication variable to

the apparatus.

75. (Previously presented) The server according to claim 69, wherein the authentication method is SecureId, SafeWord, Wireless Public Key Infrastructure (WPKI) and/or Wireless Identity Module (WIM) authentication.